Breach Fatigue:
Consumer Apathy Towards Data Breaches and Personal Security

THESIS

Presented in Partial Fulfillment of the Requirements for the Bachelor of Science in Business Administration Degree with Honors Research Distinction in the Max M. Fisher College of Business of The Ohio State University

By

Matthew Xavier Shaver

Marketing Specialization in Business Administration

The Ohio State University

2016

Dissertation Thesis Committee:

Vasu Unnava, Advisor

Patricia West, Member

Daniel Zane, Member

Matthew Xavier Shaver

2016

Abstract

In the past five years data security breaches have transformed from relatively unknown occurrences to widespread infiltrations of large corporations covered by the national media. While studies have been conducted regarding consumer sentiment after being affected by a "mega" data breach, none have attempted to understand how data breaches impact consumer behavior. The main objective of this paper is to uncover how direct or indirect experience with data breaches influences behavior. It is hypothesized that consumers who were directly impacted by data breaches will have taken the most severe steps to prevent further data security issues. A 77-question survey was created to compare behavioral actions taken by three consumer groups: those personally affected by data breaches, those indirectly affected, and those not affected. A Chi-Square analysis was conducted to determine if proportionate responses varied significantly between the groups. Results were surprising, showing that regardless of the means by which data breaches affected consumers (direct, indirect, or none) their data security behaviors remained statistically similar. This goes to show that consumers have not necessarily translated their negative past experiences with data breaches into actual behavioral changes. However, interesting findings were made with regards to how consumers use debit cards and social security numbers following a data breach. The hope is that with this information uncovered companies who provide data security services or who benefit from customers proactively securing data can better create pitches or programs that speak to behavior-indifferent consumers. This research allows for further study into the feelings and emotions that prevent consumers in these different groups from taking differing actions. It could also be replicated with the main focus on those directly impacted, and work to test ways companies can incentivize these consumers to change their behaviors for the better.

Acknowledgments

I would like to sincerely thank Dean Patricia West for the guidance and endless support she provided me with these past two years. Without her help I would not be graduating with an Honors Degree. Her personal interest in the success and long-term well being of her students is admirable to say the least. Also monumental to my success in the Honors program is Professor Vasu Unnava. Her assistance with the Consumer Packaged Goods Industry Cluster and project mentorship were both highly enjoyable and educational. Thank you Professor Unnava for all of your support and interest in my professional development. I owe thanks to Daniel Zane as well, I could not have completely my analysis without his help. I would like to thank my fellow Honors Contract class who began this journey alongside me in this first ever restructured program. Thank you for your inspiration, feedback, and research assistance, I wish you the best of luck. I would like to thank my classmates, mentors, and friends in the Alpha Kappa Psi Mu Chapter professional business fraternity. Without their continual support, motivation, and adherence to the highest ideals of education and personal accomplishment I would have never pushed myself to achieve so much during my four years at The Ohio State University. Lastly, I would like to thank my parents- Edward and Lisa Shaver. Without their unyielding love, richness in spirit, and emphasis on the importance of education I would not have become the driven young man that I am today.

Vita

June 2012 .....Rocky River High School

May 2016 .....B.S.B.A. Marketing, The Ohio State University Fisher College of Business

Fields of Study

Major Field: Business Administration

Marketing

Table of Contents

List of Figures

Chapter 1: Introduction

All of us have provided our personal information to firms that we do business with at some point in our lives. The information we provide them can be extremely personal, such as one's social security number or medical records, or less intimate, like an email account or birth date. Many times this information is provided as a requirement of employment, as a means of joining a mailing list or group, or to make an actual purchase. Interestingly, 73% of consumers are very willing to share personal information if they receive some sort of benefit in return (PwC, 2012). More often than not we are aware of when we provide this information to businesses- either because they explicitly ask for it or we knowingly submit it. However, there are instances where some people may not necessarily understand what kinds of, or how much, information they provide institutions. Situations like these can arise when consumers use a credit or debit card without knowing what type of personal information is attached to it (or how that information is used by the company), or when consumers integrate social media accounts with a digital component of a firm. This contradicts what most consumers want when it comes to their own privacy, as 90% state that controlling what information is collected about them is important (Madden, 2015). There are an innumerable amount of ways by which businesses collect personal information, and an equal number of ways that consumers supply it. Over the past few decades much of this information has been collected and

stored online, culminating in vast pools of data maintained, secured, and accessed by organizations online through servers. While the internet revolution has created cost-saving and life-changing ways to collect, share, and interpret this data it has also opened the door to those without the required credentials to do the same. When this occurs, the personal information of consumers, employees, and stakeholders is at risk.

A data breach in this scenario is defined as an outside hacker or group infiltrating the security of a company or service used by consumers in order to access the consumers' private information. This information is not public knowledge and can be used to contact, locate, or identify the individual consumer; notable examples include social security number, protected health information, credit/debit card number, and email/username and password (ITRC, 2014). A data breach constitutes as a criminal attack.

At a basic level there are different, yet very important, ways data should be secured. Data should be encrypted, backed up have limited accessibility, and the servers should be stored safely (Potter, 2009). Unfortunately the majority of organizations are already doing this, and 65% of breached firms reported that the breach circumnavigated their existing security (Ponemon Institute, 2015). There is much work that still needs to be done in the field of information security, firms are upping their spending to close the gap. Similarly, many companies utilize security measurement tools and screeners. The problem with these programs is that many do not use the same terms and protocol, and many times potential vulnerabilities can be overlooked because of this (Potter, 2009). When data is sold on the black market the price varies depending on the type of data, as

well as supply and demand factors. The most valuable data includes medical records and social security numbers (EMC Corp., 2014).

As the volume of personal information stored virtually has continued to increase, so too have the number of data breaches within the United States. Over the past 10 years the amount increased substantially, from nearly 160 breaches in 2005 to over 780 breaches in 2014 (ITRC, 2014). Leading the category for the past three years have been firms in the medical and healthcare industry, followed closely by the general business segment, and then the government/military sector (ITRC, 2014). Correspondingly, as the number of breaches increased the number of records compromised took a significant jump. However many of these more recent data breaches have compromised the information of dozens of millions of consumers in a single breach, causing them to be referred to as "Mega Data Breaches" (Ponemon Institute, 2015). Target paved the way for large scale data security issues in late 2013 when the credit and debit card information of over 40 million of its customers was stolen. Since then large firms across nearly every industry have had their security systems infiltrated, their data stolen, and their reputations impacted. Notable are large retailers like Home Depot who had 56 million card data stolen, insurance firms such as Anthem with 78 million effected parties, and America's largest financial bank, JP Morgan Chase, who saw the information of 76 million customers accessed (Ponemon Institute, 2015).

The worst case scenario that culminates from data breaches for the everyday consumer is identity theft. Identity theft, defined as the appropriation of someone else's identity to commit fraud or theft, remains as one of the fastest growing crimes in the

United States (Economist, 2001). The most common form of identity theft occurs when a person's name, address, and social security number are compromised and used to open fraudulent accounts to accrue charges and expenses without the individual's awareness. This has severe implications to the person's credit score and can result in an extremely lengthy, as well as costly, recovery process (Milne, 2003). Overall, consumers affected by identity theft may be harmed in four ways. First, by having their privacy invaded. Second, by enduring the psychological harm of their reputation being ruined. Third, by bearing the financial liability costs. And fourth, paying large transactional fees to restore their name and credit (Milne, 2003).

As more mega breaches and cases of identity theft have occurred, media coverage of data breaches has increased, perpetuating a greater awareness of breaches by consumers and organizations alike. According to the Federal Trade Commission, identity theft has remained the number one complaint by consumers for 15 consecutive years (FTC, 2015). In response, both groups have adopted methods of preparing for or responding to data breaches.

Chapter 2: Preventative Steps Taken by Consumers and Organizations

There are two possible routes taken by both consumers and organizations when it comes to data breaches- preventative and responsive. Preventative measures are those taken by consumers and organizations to minimize the risk that their personal information is ever compromised, they also serve to minimize the risk to the individual should that data be breached. Responsive measures are actions taken to minimize the risk that already compromised information can be used against the person or organization in a detrimental way. In an ideal world all groups would simply be taking preventative measures that were 100% effective. However we all know not every consumer or organization knows how to protect their information, additionally many do but simply choose not to. Even if everyone did take these protective actions there is no guarantee they will always be successful. Many times it is simply not enough, and increasingly sophisticated hackers make data security an ever-fluid challenge.

Consumers have a multitude of steps they can take to better protect their personal information. The Federal Trade Commission recommends consumers do all of the following: be alert to online impersonators, safely dispose of personal information including the safe disposal of computers and mobile devices, encrypting their data, keeping passwords private, and not over-sharing details about their lives on social media. They also encourage being extremely cautious when providing social security numbers to organizations and request consumers ask why the organization needs it, how it will be used, how they will protect it, and what happens if they don't provide their SSN. Lastly,

as a result of the increased usage of online mobile devices the FTC has tips for securing them as well. These include using an anti-virus, anti-spyware, and firewall software, being alert of phishing emails, investigating public WiFi networks before using them, locking up laptops and not saving passwords, and reading the privacy policies of websites. The last step is meant to educate consumers on how their information will be used and if it will be provided to third parties (FTC, 2012). The information collected in the survey for this research focuses primarily on password, debit card, and social security number usage, as well as personal information security systems and identity fraud insurance.

Organizations themselves can take several actions to prevent their data from being breached. However, many of these tactics are much more broad than what an individual consumer has the option to do, making them somewhat difficult to implement. One key tactic is data minimization, this involves not collecting data that is not needed, reducing the number of places where data is stored, granting employees access to sensitive data on a "as needed" basis, and removing the data responsibly once it is no longer needed. Companies also need to look beyond their IT departments when considering data security and need to keep in mind the security of third parties that they share data with, what their data loss prevention plan is in the case of an incident, and how to educate employees about appropriate handling and protection of personal data. Many organizations also decide to conduct periodic risk assessments, provide security training to all employees, retain a third-party security expert on staff, and keep up to date with security updates and encryption methods (Kroll, 2015).

Chapter 3: Reactive Steps Taken by Consumers and Organizations

Although not much research has been conducted with regard to how consumers are actually reacting to data breaches, there are a number of consistent responsive steps consumers seem to be taking- or at a least similar number of steps security experts tell them they should be taking. The first step, often times self-initiated by large banks, is replacing debit cards (Experian, 2014). Debit cards withdraw funds straight from an account, and are notoriously insecure. Combine that with the simplicity of replacing a debit card, for example walking into a JP Morgan Chase bank a receiving a new card 15 minutes later, and consumers are quick to perform this task. This step is usually combined with checking a bank statement online, as opposed to waiting to receive one in the mail, to ensure no fraudulent charges have been made (Experian, 2014). Consumers are also quick to change the passwords on their email and bank accounts following a data breach, some even opt to close emails altogether. Many experts advise never having the same password for a bank account and an email account, especially if your data may have been compromised for one or both (Experian, 2014). Again, there has not been significant research into this realm, so this study aims to help identify what other actions consumers are taking and which types of consumer groups are taking each.

What is known, however, is that in general consumers do not take much action following a security breach. Many consumers do not feel that they will be impacted by a data breach at a level that is harmful to them. Others that may feel more vulnerable

assume that credit card companies, banks, retailers, or other groups will pick up the responsibility (EMC, 2015). Consumers believe there is nothing to lose, because there seems to be zero liability, and in most cases that is what has ended up happening (O'Farrell, 2013). In addition, different groups of consumers feel that even if their information is compromised by a criminal there is not much they could do about it. The potential information struggle could last for years with the end result having the potential to be nothing of benefit (EMC, 2015). This entire consumer mindset is the basis of the "Breach Fatigue" concept that this research will apply to key learnings.

Likewise, organizations have their own ways of constructively responding to data breaches. Interestingly enough, regardless of the industry the effected companies operate in (e.g. healthcare, retail, government), most of these groups respond in similar ways. For example, a public press release is almost universally made following any data breach. However the focus of this research is primarily on large, public corporations whose data breaches impacted a very large number of consumers. Because of this the recovery and response efforts of Target, a large retail firm that suffered one of the largest data breaches to date, will be analyzed.

In 2013 Target confirmed that there had been unauthorized access to its payment card data by a third party that affected 40 million cards (FTC, 2015). Over the next year this number would grow to a possible 110 million records, making it the second largest data breach of all time (FTC, 2012). Most of the records was personal information such as name, address, and phone number, but card numbers were compromised as well. In the wake of the breach Target announced that its customers affected by the breach would

have zero liability for any fraudulent charges that arose from the breach, and established a five-part ProtectMyID program. This included a free Experian credit report, daily credit monitoring, identity theft resolution, identity theft insurance, and access to a personalized security assistance. Customers needed to self-enroll in all of these services, and they were valid for 12 months. (Kroll, 2015). Target established a website (target.com/databreach) dedicated solely to providing information, advice, and assistance to impacted customers. Articles were published on the website teaching consumers how to identify possible fraudulent charges, phishing emails, scammers. The company hired a new Chief Information Security Officer, and expedited the adoption of chip card machines in stores (Target, 2014). Despite these efforts, Target still saw sales declines for the following quarters, but eventually saw its reputation begin to recuperate (Kroll, 2015). As of 2016, the Target stock has recovered, and is around 20 points higher than its lowest point during the breach announcement (Yahoo Finance, 2016).

Chapter 4: Costs to Consumers and Organizations

As discussed previously, in many instances the costs to consumers from data breaches have been zero (O'Farrell, 2013). In today's day and age the costs associated with replacing a debit card or creating a new bank account are almost nothing, however the biggest concern to consumers comes in the form of actual identity theft. As it turns out, identity theft is easiest to perform when the person's social security number is compromised (SSA, 2015). While many consumers may feel that their social security number is safe from data breaches due to the fact that the large, well-publicized breaches are retail companies where that information is not collected, the truth is that some of the most frequently breached organizations are healthcare companies and divisions of the federal government, organizations that do store consumers SSNs (Papadimitriou, 2015). Small and midsize healthcare companies are some of the easiest targets for hackers looking to acquire robust data. The identity thieves themselves are adapting as well, using stolen information to commit crimes that are hard to detect, like tax fraud, which saw a 400% increase in the United States in 2014 (Papadimitriou, 2015). A government study conducted in 2012 found that 16.6 million people in the U.S. had their identity stolen, totaling $24.7 billion dollars in financial losses (Office of Justice Programs, Bureau of Justice Statistics, 2013). More recently, a study found that medical identity theft, which has continued to increased year by year compared to other forms, costs a typical consumer an average of $13,500 to recover from. Not only did these consumers suffer

through this financial burden, but they suffered the costs of time and energy resolving the associated issues (Medical Identity Fraud Alliance, 2015).

On that note, when data breaches occur consumers face much more than financial implications. They may experience emotional distress brought on by worrying about the safety and security of their lives. They may see their jobs and companies put at risk, as was the case when a data breach released the entire organizational structure and inner workings of Sony Pictures Entertainment- exposing the social security numbers of employees and publicizing upcoming movie productions (ITRC, 2014). Or, the information itself may be potentially more harmful than what it could be used for. Such is the case with the Ashley Madison website breach. The website's user data was hacked and released to the public, sharing the names of all who took part in the online "adulterer community" and possibly causing severe reputational harm (SSA, 2015). More recently, hackers have been focused on stealing data that makes actual crimes such as identity theft easier to commit, instead of simply going after addresses or debit cards (Papadimitriou, 2015). While it may be true that the number of compromised social security numbers has gone down in recent years, consumers cannot become complacent. While many feel that they are at no true risk of suffering personal damage after a data breach, this is not the case.

Organizations, on the other hand, have been impacted by data breaches and have felt the costs much more tangibly. Target, for example, has paid over $252 million to date to resolve the issues, liabilities, and lawsuits resulting from its data breaches. This number may seem small for a company of Target's size, and it actually is. With tax

deductions the amount spent to resolve the issue was equal to 0.1% of their 2014 sales revenue (McGinty, 2015). However, companies as large as Target are not great examples of how organizations as a whole are effected by data breaches. The Ponemon Institute found that on average, companies in the United States pay $6.5 million dollars to completely resolve a data breach. This constitutes an 11% increase from the previous year. The Institute also determined the average cost for a lost or compromised record was $217, an 8% increase (IBM & Ponemon Institute, 2015). All of these numbers are relatively small. Analysts agree that at this point in time it has been hard to see data breaches severely impact the bottom line of companies. However, experts also agree it is much more important for companies to be investing in preventative data security than to simply look at the total financial impact and shrug it off (McGinty, 2015). Besides expenses spent on rebuilding security systems and providing services to impacted consumers, organizations must also face potential costs from a loss of customers, potential litigation, potential government fines, and a decline in share value (Scott & Scott, 2011). As hackers begin focusing on stealing more valuable consumer information and continue to innovate their methods, organizations could potentially find themselves spending more and more each year on data security. More importantly, if compromised data comparable in size to the Target breach is eventually used in a way that severely impacts the well-being of consumers the results could be financially catastrophic.

What has been seen more often is the non-financial costs of data breaches to organizations. These can include, but are not limited to, tarnished public credibility, increased cost of a customer acquisition, loss of competitive advantage, increase hiring

difficulty, and a difficulty preventing further breaches (Frost). One Ponemon studies asked employees to estimate the value of their company's brand or reputation. After doing so, the diminished value of the brand was calculated as if a data breach had occurred. The resulting values were between $184 and $332 million dollars, depending on the type of data compromised (Experian, & Ponemon Institute, 2011).

Calculus on the economic impact of reputation decline from data breach	Variables	$ Millions
Average value of corporate brand or reputation	1,558	
Diminished value resulting from a data breach of customer data	21%	$332
Diminished value resulting from a data breach of employee data	12%	$184
Diminished value resulting from a data breach of IP data	18%	$281

Figure 1.

While large, well-established companies may be able to better react to these issues, small businesses cannot. 20% of data breaches impact firms with 250 or less employees (IBM & Ponemon Institute, May 2015). For a company of that size, an average cost of $200+ dollars per compromised record can mean bankruptcy. It is no wonder then that 60% of businesses this size find themselves closing within a year and a half of being impacted by a data breach (IBM & Ponemon Institute, May 2015). For these companies, the costs of data breaches are very real. And what if a company like Target were hacked again? How much lower would consumer confidence in the brand drop then? No one can say, but organizations like Target need to be prepared to respond in a way consumers understand and value regardless if it is their first data breach or fifth.

Chapter 5: The Goal of this Research

In April 2014 the Ponemon Institute published a report documenting their findings on consumer sentiment following a data breach (Ponemon Institute, 2014). The Ponemon Institute itself is "dedicated to independent research and education that advances responsible information and privacy management practices within business and government" (Ponemon Institute, 2014). Their research shed light on a previously under-studied area of data breach information- the impact of data breaches on consumers' data privacy and security concerns. Before this study, most focus had be placed on data breach prevention and response, related litigation, and the impact of data breaches on insurers and shareholders. This report shifted the focus in the direction of the consumer and their reactions to being a victim of a data breach. It identified what actions consumers' believe organizations should be taking after a data breach, how being a data breach victim impacted their concerns about identity theft, and how important victims believe media coverage of data breaches is, among other findings. This Ponemon report, along with others that the Institute published, laid the foundational work for this research.

In order to further the goal of advancing business practices with relation to information and privacy management we believed further research must be conducted to better help businesses trying to react to data breaches. We wanted to take a closer look at consumer sentiment, but focus mainly on consumer behavior with regard to data breaches. We also wanted to provide organizations a means of distinguishing amongst

different types of consumers and determine how their behaviors differ, and decided it would be most beneficial to group them by their actual experience level with data breaches. Not only would this allow us to see the behaviors of directly impacted consumers, but it would allow us to measure the data breach awareness of those not impacted and identify their behavior as well.

Put simply, the goal of this research is to provide previously unknown information on the actual behaviors of consumers with relation to data breaches. Behaviors of those directly impacted, those indirectly impact (through a spouse, for example), and those not impacted will be quantified and compared. This research opens the door to organizations being better able to respond to consumer needs following a data breach by assisting them with the behaviors they are most likely to be undertaking. Doing so minimizes unnecessary expenses and may provide long-term benefits with relation to brand reputation and customer service perceptions. It is our hope that these findings may prove useful to organizations and researchers alike.

Chapter 6: Research Methodology

Hypotheses

In order to acquire the desired information on consumer behavior with relation to data breaches, a research study had to be designed that allowed consumers to recount the actions they had taken following their involvement with a data breach. This information also needed to be gathered in a way that distinguished consumers who were directly impacted by data breaches, consumers who were indirectly impacted, and those who were never impacted. Prior to determining a way to collect the data, a hypothesis formed based on the observed natural behavior patterns of most consumers following a data security issue.

H_1: Consumers who have been directly impacted by data breaches will take more precautions to protect their personal information than consumers who have been indirectly impacted or not impacted by data breaches.

Data Collection Method

An online survey questionnaire was used to gather as much data as possible from a large number of U.S. adults in a short period of time. A 77-question survey was designed with three main parts (Appendix A). Also, depending on which of the three groups the respondents self-selected themselves into, they responded to a varying number of questions. In order to obtain a population of adults 18+ living in the United States that would respond to the whole questionnaire, Amazon Mechanical Turk was employed. 220

unique responses were generated in a period of three days, and every respondent received compensation for completing the survey.

The first part of the survey allowed respondents to self-select into one of three groups, dependent on their past experience with data breaches, and asked them specific questions corresponding to the group they fit into. The three groups were consumers who were Personally Affected, Indirectly Affected, or Not Affected by data breaches. These groups were determined through the following question.

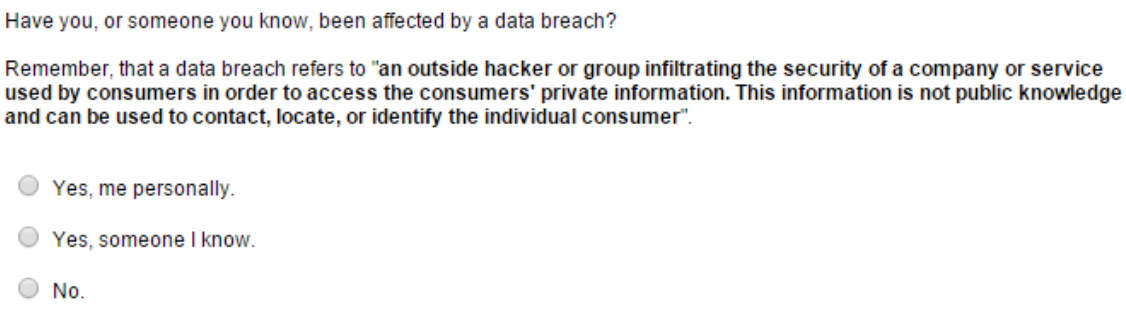

Figure 2.

Once divided into groups respondents answered questions more specific to their previous experience. For example, consumers who were directly impacted received questions about how many time they had been affected, what services the firm offered them (if any), and how satisfied they were with the way the company handled the breach. Respondents who were indirectly impacted were asked about any information they knew about the breach through questions extremely similar to those asked of the first group. Those not impacted were asked questions about if and how they have heard about data breaches, what types of organizational data breaches they were familiar with, and their opinions on the importance of knowing about breaches. The group-specific questions

were meant to be comparable in analysis, but could clearly not be the same based on differences in previous experience.

The second part of the survey was focused on consumers' knowledge of data breaches, their perception of risks associated with data breaches and security, and their behavior. All three groups of respondents received the same exact questions in these categories. The knowledge-focus questions pertained to how respondents heard about data breaches, how many different instances they had heard of, and asked them to recount any major breaches they were familiar with. The perception of risk section asked respondents how vulnerable, concerned, threatened, etc. they felt by hackers/breachers, how at risk they felt to identity theft, and whether or not they believed it was possibly to prevent data breaches entirely. Lastly, behavioral questions relating to the usage and maintenance of passwords, debit cards, and social security numbers were requested. These questions were the focal point of the research. Respondents were required to admit any steps they had taken to prepare themselves in case of a data breach, if they use a personal information security system, and if they feel protected from identity theft. Important to note is that many of these questions ask consumers whether or not they took a certain action such as changing their passwords regularly, and if they do follows up by asking whether or not they began that behavior after hearing about data breaches.

The final portion of the survey was a standard demographic analysis of the survey respondents (Appendix A). This section was meant to determine that the survey respondents represented a diverse group of consumers as well as to allow further comparison of knowledge, perception, and behavior amongst different demographic

groups with regard to data breaches and security. Respondents were asked their gender, age, household income range, highest level of education, ethnicity, marital status, and region of residence. In addition, in this section consumers were also asked if they had identity fraud insurance and if they, themselves, or a direct family member was an identity theft victim. These final questions were somewhat more personal and although no responses could be traced back to an actual individual it was our belief that they belonged among the demographic items.

Chapter 7: Findings & Conclusions

Findings on Consumer Behavior

Survey respondents were asked a number of questions related to their security behaviors. Respondents were asked whether they took certain security precautions, and if they answered affirmatively they were asked a follow-up question to determine whether or not this behavior was the result of their exposure to data breaches. For the yes/no questions (e.g. "Do you change your passwords regularly?") a Chi-Square analysis was performed to measure if there were any statistically significant differences among the three respondent categories. The statistical outputs of these tests are shown in Appendix B. The image below summarizes the findings (Figure 3).

Question	Chi-Square Analysis
Do you change your passwords regularly?	No statistical difference between the three groups.
Do you use debit cards regularly?	No statistical difference between the three groups.
Do you provide companies with your SSN regularly?	Statistically significant differences between groups.
Do you use a personal data security service or program?	No statistical difference between the three groups.

Figure 3.

According to the Chi-Square analysis consumers exhibit the same current behaviors with regards to changing passwords, using debit cards, and using a personal data security service regardless of whether they were directly, indirectly, or not impacted by data breaches. This evidence suggests that experience with data breaches, both first-hand or indirectly, does not necessarily translate into taking personal information security precautions. The analysis discovered that consumer behaviors with regard to social

security numbers do vary across groups. More interestingly, consumers who have been directly impacted by data breaches showed the highest proportionate willingness to provide companies with their SSNs.

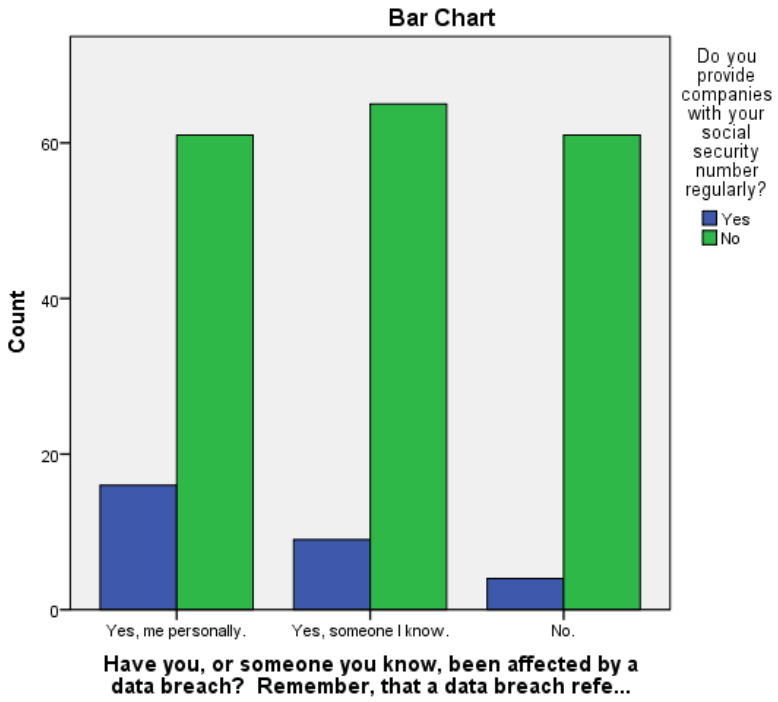

Figure 4.

This is intriguing due to the fact that this question is determining current behavior, meaning that even after being affected by a data breach these respondents were still willing to regularly give companies one of the most personal pieces of private information available in this country. While only 20.8% of those directly impacted stated that they provide SSNs regularly, this was significantly higher than those indirectly impacted (12.2%) and those not impacted (6.2%). Also noteworthy is the fact that those who had never been impacted by data breaches in any way are the least likely to give out their social security number.

More important than these questions were the follow up ones asked to determine whether or not the current behavior exhibited by respondents was the result of being influenced by a data breach. A different approach was used to analyze these secondary questions. For each set of two questions, responses were categorized into No (respondents answered that they did not undertake a particular behavior), Yes/No (respondents answered that they did undertake a particular behavior but it was not a result of hearing about data breaches), and Yes/Yes (respondents answered that they did undertake a particular behavior as a result of hearing about data breaches). These options were different for the question pertaining to social security numbers and whether or not they use a personal data security service. Appendix A contains the wording of all survey questions for reference.

The summary of these findings can be seen in Figure 5.

Passwords	Y/Y	Y/N	N	Total # That Changed Behavior	% That Changed b/c of Data Breach
Directly	27	16	34	43	63%
Indirectly	25	15	34	40	63%
Not Impacted	24	12	29	36	67%
Debit Cards	Y/Y	Y/N	N	Total # That Changed Behavior	% That Changed b/c of Data Breach
Directly	15	9	28	24	63%
Indirectly	10	13	28	23	43%
Not Impacted	3	11	30	14	21%
SSN	N/Y	N/N	Y	Total # That Changed Behavior	% That Changed b/c of Data Breach
Directly	3	58	16	61	5%
Indirectly	5	60	9	65	8%
Not Impacted	5	56	4	61	8%
Security Service	Y/Y	Y/N	N	Total # That Changed Behavior	% That Changed b/c of Data Breach
Directly	6	11	60	17	35%
Indirectly	11	5	58	16	69%
Not Impacted	5	2	58	7	71%

Figure 5

These findings, while not the result of statistical modeling, tell an interesting story. With regards to password and social security behaviors consumers seem to maintain similar

behaviors regardless of whether they were directly, indirectly, or not impacted by a data breach. 63%, 63%, and 67% (respectively) of respondents in the three groups who change their passwords regularly do so because they were influenced by hearing about data breaches. Looking at social security number usage, 5%, 8%, and 8% of respondents who do not regularly provide companies with their social security number stated that they do not because they were impacted after hearing about data breaches. While these percentages show that data breaches had more of an impact on behaviors related to passwords than they did on those related to SSNs, they also fail to show any major differences between the three respondent categories. However, the story about debit card and private data security program usage is somewhat different. 63% of directly impacted respondents took debit card security measures as a result of hearing about data breaches, 43% of indirectly impacted respondents took debit card security measures as a result of hearing about data breaches, and for those not impacted the rate was 21%. These results are the most supportive of what this research hypothesized- that consumers directly impacted by data breaches would take more precautions with regards to data security behaviors than consumers indirectly impacted or not impacted. This result makes sense, as many consumers who were impacted may have been involved in one of the large mega breaches and may have been automatically issued a new debit card by their bank. The same breakdown was found with regards to respondents who use a personal data security program or service. 65% of directly impacted respondents began using a data security service after hearing about data breaches, 31% of indirectly impacted respondents began using a data security service after hearing about data breaches, and for those not impacted

the rate was 29%. What this means is that those directly impacted were much more likely to then begin using a data security service, which again makes sense. While this information is obvious and useful to the companies that provide these services, it is interesting to note that nearly one third of people indirectly impacted and not impacted at all have acquired these same services due simply to hearing about data breaches. Targeted marketing efforts could be utilized to better reach these segments and offer them the same products that are currently being sold to people who have experienced a data breach. The breakdown percentages found for debit cards and data security services are what we expected for all of the behavior-based questions, but that was simply not the result.

Findings on Consumer Sentiment

Respondents were asked questions relating to their current feelings with regards to data breaches. These eight questions pertained to items such as perceived safety, vulnerability, concern over identity theft, preparedness, and perceptions of companies. While these questions were not the main focus of the research, a statistical analysis was still run on their results so that they may prove useful in further research pertaining to consumers and data breaches. The questions measuring perceived safety, threat, vulnerability, and concern were asked on as scale questions, and therefore an ANOVA test was run to determine if there were significant differences among the groups. The findings can be seen in Figure 6.

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
How safe do you feel your personal information is at this moment in time?	Between Groups	3.199	2	1.600	3.634	.028
	Within Groups	93.759	213	.440		
	Total	96.958	215			
How threatened do you feel by hackers/data breachers at this moment in time?	Between Groups	3.058	2	1.529	2.625	.075
	Within Groups	124.035	213	.582		
	Total	127.093	215			
How vulnerable to identity theft do you feel at this moment in time?	Between Groups	2.519	2	1.260	2.725	.068
	Within Groups	98.476	213	.462		
	Total	100.995	215			
In general, how concerned are you about identity theft?	Between Groups	1.892	2	.946	.749	.474
	Within Groups	269.067	213	1.263		
	Total	270.958	215			

Figure 6.

The results show statistically significant differences between groups only for the question pertaining to perceived safety, at a 99.95% confidence level. However, if the confidence level were to be 99.90%, the questions pertaining to safety, threat, and vulnerability would all be statistically different between groups. Moreover, the directionality shows that consumers who were directly impacted by data breaches were also the ones that felt the most vulnerable, concerned, threatened, and unsafe (Appendix C). There is a clear disconnect here between the emotions and behaviors of respondents. Differences in these perceived feelings are not being translated into action. With regards to the question about identity theft concern, there appears to be no differences between groups.

Lastly, three yes/no questions related to consumer beliefs were asked. They pertained to the possibility of companies preventing data breaches, a company they do business with having their data breached in the near future, and feelings of preparedness should a data breach effect them. A Chi-Square test was run on the results of these three questions and provided one statistically significant response. When asked whether they

thought a company that they currently do business with will have their data breached in the near future, respondents who had been personally effected by a data breach responded "yes" proportionately more than respondents who had never been effected by a data breach (Figure 7). The Chi-Square analysis revealed an approximate significance of 0.005.

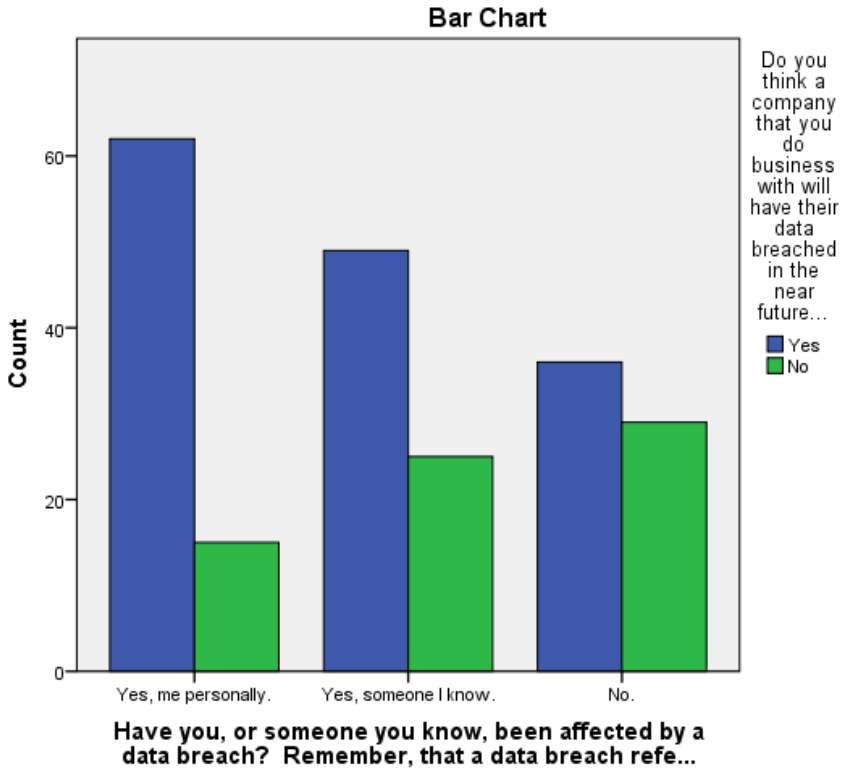

Figure 7.

This result is not astounding, however, as it can be expected that consumers who themselves have been impacted by a data breach are more likely to believe another company will have their data breached in the near future due to cognitive biases. Overall, these findings just scratch the surface of consumer beliefs, feelings, and emotions with regards to data breaches. Further research could provide more in-depth rationale as to

why this disconnect between thought and action exist and how, if at all, it puts consumers and their information security at risk. Lastly, further research and concept testing could be conducted by companies to assess what types of incentives or procures would be the most effective at translating these negative consumer fears into proactive data protection actions. For example, companies could test out requiring their consumers to change passwords every six months, or they could offer a slight discount if consumers used credit cards instead of debit cards.

This journal cannot claim that there are substantial differences between behaviors among consumers who have experienced data breaches directly, indirectly, or not at all. While some variation exists between for questions pertaining to specific pieces of information, the overall message is one of consumer apathy towards data security. There is not convincing evidence to suggest data security behaviors vary amongst the three tested groups of consumers.

Discussion and Conclusion

There were several limitations to this research. First, the sample used was confined only to U.S. adults that were current users on Amazon's Mechanical Turk service. This limits the population sample to adults that have an internet access and are actively seeking surveys to participate in for monetary compensation. While the responses we received were from a somewhat diverse group when it came to items like income, geography, and marital status, among others, 81% of the responses were from Caucasians. These results underrepresented minority groups greatly. Another possible flaw with the survey is that for 73% of respondents there was zero financial cost for them

to fix the data breach problems. It is intriguing to think how the behaviors may have varied more had more consumers with larger negative financial outcomes participated. Additionally, the wording of many of the behavioral questions prompted respondents to describe their behavior before and after "hearing" about data breaches. This wording was vague and could very easily be interpreted differently among the three respondent groups. Another issue with wording arose when respondents were asked whether or not they were "glad" to have heard about data breaches. Many respondents took this as meaning they derived pleasure from hearing about other people suffering from data breaches, which was not the intention of the questions. Also, some questions asked respondents to describe behaviors they used to undertake, whenever this is done there is a strong chance that consumers may state was they did incorrectly, unintentionally. Furthermore, this entire survey was in English. The United States is a country populated by many non-native English speakers and people for whom English is not their primary language. It would be negligent to apply these findings to groups of non-English speaking people. Lastly, there were no statistical tests run on the questions that were meant to determine why a respondents behavior was or was not changed. For the sake of this research, the proportions and percentages calculated proved enough to show that had any statistical tests been run they would most likely had not yielded any sort of information that would prove staunch differences in behaviors between groups- at least no consistent findings. Further research may benefit from using further statistical analysis should this same area of consumer behavior be examined.

This journal has the potential to lead to future data breach-related consumer behavior research. It may be useful to duplicate this research, but with a more strict focus on behavior. It would also be better if a more diverse sample is questioned. The findings were drawn only from an online survey, but combining these with individual interviews, focus groups, and other forms of research may provide further insight into why many consumers have decided to take similar actions with regard to data security. In addition, further research comparing the behaviors of consumers impacted by different types of breaches (ex. retail breach versus government breach) could provide interesting behavioral differences. The same can be said of interviewing more consumers who had large financial or legal implications as a result of their data breach, and uncovering how their behaviors before and after the event may compares to the behaviors of those never impacted by a breach. Lastly, with these findings showing that consumer behavior does not differ much between consumers who experience data breaches directly, indirectly, or not at all, organizations can work to provide services that appeal to everyone, as opposed to more targeted methods.

References

1. ITRC. (2014). Data Breach Reports (pp. 1-192, Rep.). Retrieved April 1, 2015, from ITRC website: http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html

2. Ponemon Institute. (2015, January). 2014: A Year of Mega Breaches (Rep.). Retrieved April 1, 2015, from Ponemon Institute LLC website: http://www.ponemon.org/local/upload/file/2014 The Year of the Mega Breach FINAL3.pdf

3. PwC. (2012). The speed of life: Consumer intelligence series (pp. 1-11, Rep.). PricewaterhouseCoopers LLP. Retrieved December 26, 2015, from http://www.pwc.com/us/en/industry/entertainment-media/assets/pwc-consumer-privacy-and-information-sharing.pdf

4. Madden, M., & Rainie, L. (2015, May 20). Americans' Attitudes About Privacy, Security and Surveillance. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

5. Potter, B., Harauz, J., & Kaufman, L. (2009). Data Security in the World of Cloud Computing. *IEEE Security & Privacy,* 61-64.

6. EMC Corporation & Ponemon Institute (2014). Consumer Perceptions on Security: Do They Still Care? Retrieved from http://www.emc.com/collateral/brochure/consumer-perceptions-on-security.pdf

7. *Economist.* 2001. United States: Stealing People is Wrong. *The Economist,* 358 (8212): 28-29. (Economist, 2001)

8. Milne, G. R. (2003). How Well Do Consumers Protect Themselves from Identity Theft?. Journal Of Consumer Affairs, 37(2), 388-402.
(Milne, 2003)

9. FTC. (2015, February 27). *Identity Theft Tops FTC's Consumer Complaint Categories Again in 2014* [Press release]. Retrieved from https://www.ftc.gov/news-events/press-releases/2015/02/identity-theft-tops-ftcs-consumer-complaint-categories-again-2014

10. FTC. (2012, July). How to Keep Your Personal Information Secure. Retrieved from https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure

11. Kroll. (2015). Data Breach Prevention Tips. Retrieved from http://www.kroll.com/en-us/cyber-security/data-breach-prevention/cyber-risk-assessments/data-breach-prevention-tips

12. Target. (2014, April 29). *Target Appoints New Chief Information Officer, Outlines Updates on Security Enhancements* [Press release]. Retrieved from https://corporate.target.com/press/releases/2014/04/target-appoints-new-chief-information-officer-outl

13. Yahoo Finance. (2016). *TGT: Target Corp.* (Rep.). Retrieved from http://finance.yahoo.com/q?s=TGT

14. Experian. (2014). *Data Breach Response Guide* (pp. 1-31, Rep.). Retrieved from https://www.experian.com/assets/data-breach/brochures/response-guide.pdf.

15. EMC. (2015). Retrieved from http://www.emc.com/collateral/brochure/consumer-perceptions-on-security.pdf

16. O'Farrell, N. (2013, August 26). 12 Reasons Why We're Losing the Battle Against Identity Theft [Web log post]. Retrieved from http://idt911.com/education/blog/12-reasons-why-were-losing-the-battle-against-identity-theft

17. SSA. (2015). *Identity Theft and Your Social Security Number* (pp. 1-8, Rep.). Social Security Administration. Retrieved from https://www.ssa.gov/pubs/EN-05-10064.pdf.

18. Papadimitriou, O. (2015). Identity Theft: What It Is, How It Happens & the Best Protection. Retrieved from https://wallethub.com/edu/identity-theft/17120/

19. Office of Justice Programs, Bureau of Justice Statistics. (2013, December 12). *16.6 MILLION PEOPLE EXPERIENCED IDENTITY THEFT IN 2012* [Press release]. Retrieved from http://www.bjs.gov/content/pub/press/vit12pr.cfm

20. Medical Identity Fraud Alliance, & Ponemon Institute. (2015, February). *Fifth Annual Study on Medical Identity Theft* (Rep.). Retrieved from http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf

21. McGinty, K. (2015, February 26). Target Data Breach Price Tag: $252 Million and Counting | Privacy & Security Matters. Retrieved from https://www.privacyandsecuritymatters.com/2015/02/target-data-breach-price-tag-252-million-and-counting/

22. IBM, & Ponemon Institute. (2015). *2015 Cost of Data Breach Study: United States* (Rep.). Retrieved http://www-03.ibm.com/security/data-breach/

23. Scott & Scott. (2011). Scott Technology Attorneys. Retrieved from http://www.scottandscottllp.com/main/business_impact_of_data_breach.aspx

24. Frost, S. (n.d.). Retrieved from http://www.faronics.com/assets/White-Paper-Small-businesses-face-failure-through-data-breaches.pdf

25. IBM, & Ponemon Institute. (2015, May). *2015 Cost of Data Breach Study: Global Analysis* (Rep.). Retrieved https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

26. Experian, & Ponemon Institute. (2011, November). *Reputation Impact of a Data Breach: U.S. Study of Executives & Managers* (Rep.). Retrieved https://www.experian.com/assets/data-breach/white-papers/reputation-study.pdf

27. Ponemon Institute (2014, April). *The Aftermath of a Data Breach: Consumer Sentiment* (Rep.). Retrieved http://www.ponemon.org/local/upload/file/Consumer Study on Aftermath of a Breach FINAL 2.pdf

Appendix A: Survey Questions & Results

1. Have you, or someone you know, been affected by a data breach? Remember, that a data breach refers to "an outside hacker or group infiltrating the security of a company or service used by consumers in order to access the consumers' private information. This information is not public knowledge and can be used to contact, locate, or identify the individual consumer".

#	Answer		Response	%
1	Yes, me personally.		79	36%
2	Yes, someone I know.		75	34%
3	No.		66	30%
	Total		220	100%

2. How many data breaches notifications have you received within the past three years? Please answer this question based on the number of notifications about different data breaches, not multiple notifications of the same data breach.

#	Answer		Response	%
1	0		2	3%
2	1		31	40%
3	2		31	40%
4	3		10	13%
5	4		4	5%
6	5		0	0%
7	More than 5		0	0%
	Total		78	100%

3. When were you affected by the data breach? (If you were affected by multiple data breaches please choose the time period of the most recent data breach.)

#	Answer		Response	%
1	Within the past year		38	49%
2	Between 1 and 3 years ago		38	49%
3	Between 3 and 4 years ago		0	0%
4	More than 4 years ago		2	3%
	Total		78	100%

4. Were you aware of data breaches before you were personally affected by one?

#	Answer		Response	%
1	Yes		65	83%
2	No		13	17%
	Total		78	100%

5. What type of organization was your data breached from? Please select all that apply.

#	Answer		Response	%
1	Airline		0	0%
2	Bank		16	21%
3	Cable Company		1	1%
4	Catalogue		2	3%
5	Charity		1	1%
6	Court/Public Records		3	4%
7	Credit Card Company		10	13%
8	Drug Store		0	0%
9	Gaming		6	8%
10	Grocery Store		3	4%
11	Hospital / Clinic		1	1%
12	Hotel		2	3%
13	Information Broker		0	0%
14	Insurance Company		7	9%
15	Internet Provider		2	3%
16	Financial Advisor		0	0%
17	Law Enforcement		0	0%
18	Retail Store		35	45%
19	School / University		3	4%
20	Social Media		3	4%
21	State / Local Government Agency		12	15%
22	Telephone Provider		3	4%
23	Web Retailer		4	5%
24	Other (please specify)		6	8%

Other (please specify)
Yahoo
Federal Government
Email
email
federal government
My email was hacked

6. Were you provided details about what kind of information was compromised by the data breach?

#	Answer		Response	%
1	Yes		62	79%
2	No		16	21%
	Total		78	100%

7. What kind of information was compromised by the data breach? Please select all that apply.

#	Answer		Response	%
1	Name		45	74%
2	Address		36	59%
3	Email address		24	39%
4	Telephone Number		20	33%
5	Age / DOB		19	31%
6	Gender		19	31%
7	Employer		6	10%
8	Insurance Number		4	7%
9	CVV from Credit Card		10	16%
10	Credit Card or Bank Payment Information		30	49%
11	Credit or Payment History		3	5%
12	Password / PIN		7	11%
13	Social Media Account		1	2%
14	Health Plan Provider / Account Number		2	3%
15	Taxpayer ID Number		0	0%
16	Social Security Number (SSN)		21	34%
17	Other (please specify)		0	0%
18	Don't Know		5	8%

8. What was the financial cost necessary to fix the consequences of the data breach?

#	Answer		Response	%
1	Zero		56	73%
2	Less than $10		3	4%
3	Between $10 and $100		8	10%
4	Between $100 and $500		3	4%
5	Between $500 and $1000		1	1%
6	Greater than $1000		6	8%
	Total		77	100%

9. How much time did you spend resolving the problems associated with the data breach that affected you?

#	Answer		Response	%
1	1 day		39	51%
2	1 week		17	22%
3	1 month		9	12%
4	3 months		4	5%
5	6 months		1	1%
6	1 year		0	0%
7	More than 1 year		0	0%
8	Never fully resolved		7	9%
	Total		77	100%

10. Did you experience an increase in stress after being notified about the data breach?

#	Answer		Response	%
1	Yes		50	65%
2	No		27	35%
	Total		77	100%

11. Was a lawsuit filed against the company after the data breach incident occurred?

#	Answer		Response	%
1	Yes		5	6%
2	No		26	34%
3	I do not know		46	60%
	Total		77	100%

12. Did you receive any form of compensation from the lawsuit?

#	Answer		Response	%
1	Yes		2	40%
2	No		3	60%
	Total		5	100%

13. Did the company cease operations as a result of the data breach?

#	Answer		Response	%
1	Yes		0	0%
2	No		73	95%
3	I do not know		4	5%
	Total		77	100%

14. Did you discontinue your relationship with the company after the data breach?

#	Answer		Response	%
1	Yes		18	23%
2	No		59	77%
	Total		77	100%

15. After hearing about the data breach, did you do any of the following: Please select all that apply.

#	Answer		Response	%
1	Contacted the company directly		23	33%
2	Visited a company web page related to the breach		38	54%
3	Contacted your personal bank		27	39%
4	Searched for additional information online		41	59%
5	Searched for additional information on news media (TV, Radio, Newspaper/Magazine)		10	14%

16. Did the company offer any of the following services after the data breach:Please select all that apply:

#	Answer		Response	%
1	A personal apology (not generic)		23	36%
2	Discounts		5	8%
3	Gift cards		3	5%
4	Access to a call center		6	9%
5	Access to an informational web page		20	31%
6	Free identity theft protection		34	53%
7	Free credit monitoring service		33	52%

17. Do you agree or disagree that there was sufficient communication from the company to you about the data breach?

#	Answer		Response	%
1	Strongly Disagree		6	8%
2	Disagree		16	21%
3	Neither Agree nor Disagree		21	27%
4	Agree		30	39%
5	Strongly Agree		4	5%
	Total		77	100%

18. Overall, how satisfied were you with the way the company reacted to the data breach?

#	Answer		Response	%
1	Very Dissatisfied		6	8%
2	Dissatisfied		17	22%
3	Neutral		26	34%
4	Satisfied		23	30%
5	Very Satisfied		5	6%
	Total		77	100%

19. How confident are you that the company will not have its data breached again?

#	Answer		Response	%
1	Extremely confident		2	3%
2	Very confident		6	8%
3	Somewhat confident		23	32%
4	Not very confident		22	30%
5	Not at all confident		20	27%
	Total		73	100%

20. Do you agree or disagree that you are more knowledgeable about how to protect your information now that the data breach has occurred?

#	Answer		Response	%
1	Strongly Disagree		2	3%
2	Disagree		10	13%
3	Neither Agree nor Disagree		27	35%
4	Agree		33	43%
5	Strongly Agree		5	6%
	Total		77	100%

21. Are you happy with the reactive steps you took following the data breach?

#	Answer		Response	%
1	Very Unhappy		0	0%
2	Unhappy		3	4%
3	Neither Happy nor Unhappy		25	32%
4	Happy		44	57%
5	Very Happy		5	6%
	Total		77	100%

22. Who was effected by the data breach? Please select all that apply.

#	Answer		Response	%
1	Spouse		2	3%
2	Parent		17	23%
3	Child		2	3%
4	Neighbor		7	9%
5	Close Family Friend		19	26%
6	Relative (other)		13	18%
7	Coworker		13	18%
8	Acquaintance		13	18%
9	Other (please specify)		2	3%

Other (please specify)
Fiancee
Lifelong friend

23. How many people that you know personally have been affected by a data breach?

#	Answer		Response	%
1	1		42	57%
2	2		24	32%
3	3		3	4%
4	4		2	3%
5	5 or more		3	4%
	Total		74	100%

24. When was this person most recently affected by a data breach?

#	Answer		Response	%
1	Within the past year		33	45%
2	Between 1 and 3 years ago		31	42%
3	Between 3 and 4 years ago		4	5%
4	More than 4 years ago		5	7%
	Total		73	100%

25. What type of company had its data breached? Please select all that apply.

#	Answer	Response	%
1	Airline	0	0%
2	Bank	22	30%
3	Cable Company	1	1%
4	Catalogue	0	0%
5	Charity	0	0%
6	Court/Public Records	0	0%
7	Credit Card Company	18	24%
8	Drug Store	1	1%
9	Gaming	4	5%
10	Grocery Store	5	7%
11	Hospital / Clinic	2	3%
12	Hotel	0	0%
13	Information Broker	0	0%
14	Insurance Company	1	1%
15	Internet Provider	1	1%
16	Financial Advisor	1	1%
17	Law Enforcement	0	0%
18	Retail Store	23	31%
19	School / University	1	1%
20	Social Media	6	8%
21	State / Local Government Agency	3	4%
22	Telephone Provider	3	4%
23	Web Retailer	1	1%
24	Other (please specify)	5	7%

Other (please specify)
It was never determined how the information was obtained
Federal Government
health clinic
IRS
restaurant

26. Was the person affected by any of the following large data breaches? Please select all that apply.

#	Answer		Response	%
1	Target		27	40%
2	JP Morgan Chase		7	10%
3	The Home Depot		1	1%
4	Snapchat		2	3%
5	Sony		1	1%
6	Nationwide Mutual Insurance		0	0%
7	Walgreens		0	0%
8	Facebook		4	6%
9	LinkedIn		0	0%
10	Adobe		0	0%
11	Twitter		1	1%
12	Ashley Madison		0	0%
13	Google Chrome		0	0%
14	None of the above		28	41%

27. Do you know what type of information was compromised by the data breach? Please select all that apply.

#	Answer		Response	%
1	Name		40	65%
2	Address		29	47%
3	Email address		23	37%
4	Telephone Number		22	35%
5	Age / DOB		27	44%
6	Gender		19	31%
7	Employer		9	15%
8	Insurance Number		4	6%
9	CVV from Credit Card		18	29%
10	Credit Card or Bank Payment Information		38	61%
11	Credit or Payment History		9	15%
12	Password / PIN		11	18%
13	Social Media Account		5	8%
14	Health Plan Provider / Account Number		2	3%
15	Taxpayer ID Number		2	3%
16	Social Security Number (SSN)		13	21%
17	Other (please specify)		2	3%

Other (please specify)
paypal
Steam account

28. What was the financial cost necessary to fix the consequences of the data breach?

#	Answer		Response	%
1	Zero		25	38%
2	Less than $10		3	5%
3	Between $10 and $100		3	5%
4	Between $100 and $500		13	20%
5	Between $500 and $1000		3	5%
6	Greater than $1000		3	5%
7	There were some, but I do not know the amount		15	23%
	Total		65	100%

29. How much time did they spend resolving the problems associated with the data breach?

#	Answer		Response	%
1	1 day		11	17%
2	1 week		22	35%
3	1 month		16	25%
4	3 months		9	14%
5	6 months		1	2%
6	1 year		1	2%
7	More than 1 year		3	5%
8	Never fully resolved		0	0%
	Total		63	100%

30. Did they experience an increase in stress after hearing about the data breach?

#	Answer		Response	%
1	Yes		66	93%
2	No		5	7%
	Total		71	100%

31. Was a lawsuit filed against the company after the data breach incident occurred?

#	Answer		Response	%
1	Yes		2	5%
2	No		41	95%
	Total		43	100%

32. Did they receive any form of compensation from the lawsuit?

#	Answer		Response	%
1	Yes		2	100%
2	No		0	0%
	Total		2	100%

33. Did the company cease operations as a result of the data breach?

#	Answer		Response	%
1	Yes		1	1%
2	No		67	99%
	Total		68	100%

34. Did they discontinue their relationship with the company after the data breach?

#	Answer		Response	%
1	Yes		7	11%
2	No		56	89%
	Total		63	100%

35. Did you know what a data breach was prior to being exposed to this survey?

#	Answer		Response	%
1	Yes		63	95%
2	No		3	5%
	Total		66	100%

36. How have you heard about data breaches? Please select all that apply.

#	Answer		Response	%
1	Radio		17	27%
2	Television		45	71%
3	Newspapers		18	29%
4	Internet		58	92%
5	Social Media		32	51%
6	Other people		29	46%
7	Other		3	5%

37. How frequently have you heard or read about a data breach reported in the media in the past three years?

#	Answer		Response	%
1	None		0	0%
2	1 to 2 times		10	17%
3	3 to 5 times		26	44%
4	More than 6 times		23	39%
	Total		59	100%

38. What types of organizations/companies do you remember having their data breached? Please select all that apply.

#	Answer	Response	%
1	Airline	5	8%
2	Bank	28	44%
3	Cable Company	8	13%
4	Catalogue	2	3%
5	Charity	6	10%
6	Court/Public Records	9	14%
7	Credit Card Company	31	49%
8	Drug Store	6	10%
9	Gaming	17	27%
10	Grocery Store	8	13%
11	Hospital / Clinic	9	14%
12	Hotel	4	6%
13	Information Broker	1	2%
14	Insurance Company	5	8%
15	Internet Provider	8	13%
16	Financial Advisor	3	5%
17	Law Enforcement	8	13%
18	Retail Store	49	78%
19	School / University	12	19%
20	Social Media	19	30%
21	State / Local Government Agency	15	24%
22	Telephone Provider	7	11%
23	Web Retailer	18	29%
24	Other (please specify)	9	14%

Other (please specify)
Online dating site
Sony
IRS
Kids toy tablets
Ashley Madison
Federal Government Agency
federal goverment agency
Sony
Sony

39. Are you glad you heard about data breaches although you were unaffected?

#	Answer		Response	%
1	Yes		47	75%
2	No		5	8%
3	Indifferent		11	17%
	Total		63	100%

40. Please explain why you are glad to have heard about data breaches in the space below.

Text Response
It helps me to try to keep my data safe.
Makes me more vigilant to protect my identity
To know what to look for if it happens to me and to understand it better making me more aware.
It helps me realize that you can never be too careful and to take precautions on the Internet with sensitive information.
I think it's good because it gives a head up to potential breached costumers of said company.
because it is useful in future security purpose
It lets me know I should keep my guard up.
I'd like to know how it happened and how I can protect myself against it in the future .
It is important to know what the risks are out there and what is happening as a result of said risks.
Just the fast that I know there is suspicous activity going on and to stay vigilant on my financial information.
Despite the problems the victims of data breaches may have, I feel that learning about details and methods can help future people to avoid data breaches. I think that this problem being made public will help strengthen security on the matter and allow people to take the proper measures to avoid damage of data breaches.
I'm glad I heard about them because it allowed me to check and make sure I hadn't been affected. It also makes me trust the companies more when they come out about these things.
It makes me aware of the potential risks involved with personal information
glad to keep myself informed
It's important to know about whats going on in the world around you and also so you can try and protect yourself against things like this.
It helps me to be aware of what is going on, and keep me on my toes, per say, as to what I share.
I like to be aware of what is going on around me and of things that could possibly concern me. I do a ton of shopping online and usually the news reports about data breaches gives some information on how you can safeguard yourself best. I know this doesn't help when a company is breached but it does make me aware of small steps I can take myself.
I can be more aware of these actions and try and be more careful
Interesting.
Being informed on this problem allows me to protect myself from it before it becomes and issue to me personally.
The more I am informed and educated the less likely I am to be a victim of a data breach.
Now that I am aware I won't be so shocked when/if it ever happens to me and I hope I'm prepared for it.
It is good to be aware of potential risks and what has been targeted.
So I am aware of what retailers may have insufficient information security.
Because it helps me to be aware of the possibility of a data breach, and how to possibly protect myself. If nothing else, news of the data breach informs me not to pay for things at that particular retailer using a credit card.
A lot of data breaches go without any media coverage
I am glad to be informed of them when they happen in order to access risk for myself in the future and build awareness.
I am glad to have heard about the data breaches because it made me more aware of the problem and encouraged me to be more careful when giving information to companies and organizations both online and in person. It also reassured me somewhat that the companies were keeping a close watch in that they caught the data breaches in a relatively short amount of time before even greater damage was done.
You never know, better to hear about it than not know and might be affected.
I'd rather have companies admit they were breached than try to hush it up. It also gives you the opportunity to see if you were affected.
I need to be aware that the problem exists so I can attempt to protect myself.
It lets me know that they at least detected it instead of it being some secretive nightmare.
I am glad I heard about it, so that I won't be so callous in handling my own information. There is nothing wrong with a wake up call so people realize that this activity is real and can happen to anyone and that you should stay alert and aware.
So I can be prepared if it happens to me

When I use a service or have an account with an organization that is involved in a data breach, I can go and change my account login credentials or close my account entirely. I have the power to avoid some further damage.	
I'm glad because it reminds me to periodically update my passwords and not fall for any of the common scams, especially online.	
It gives me greater awareness of what is going on in terms of how information from consumers, students and employees are used during a breach. In addition, it allows various institutions to develop more secure networks to prevent future occurrences of data breach.	
I am glad so that I can look into my finances to make sure that I have not been involved	
It alerts me to a present danger. It makes me more aware of dangers and I then learn how I may avoid them.	
I'm glad to hear about the data breaches so I can know if it effects me or not.	
Because it could happen to anyone.	
I am glad to have heard of data breaches because it makes me more cautious in trying to avoid it myself.	
Being made aware of ongoing cyber threats allows me to better protect myself from various outside sources.	
Because it makes me aware that it could happen	
I was glad to hear about data breaches because it brought to my attention the possibility of it happening and that online/physical stores and business are not prepared to safeguard against it.	
It helps keep me in the know. Whether I was affected or not, I think it allows me to better be aware of potential dangers.	
Total Responses	46

41. Please explain why you are not glad to have heard about data breaches in the space below.

Text Response
It is an invasion of privacy to be a victim of a data breech. I'm not glad to here about that happening to anyone.
I do not like hearing about news that cause other people harm.
Hmmmm -- not sure exactly what you mean about being "gald to hear about data breaches". I am not glad to hear that other people have suffered due to data breaches -- that's what I was thinking when I answered the question. But, in rereading it I realize that I am glad to have been informed that data breaches occurred so that I might take steps to protect myself -- although I can't imagine what I can do.
I don't like reading about innocent people having their identity exposed or used for fraudulent reasons. It's good data breach is brought to the public attention but I wish such incidents never existed.
Because I'm generally not sadistic. Hearing about other peoples' misfortune usually doesn't make me glad.

42. In your opinion, which type of incident would have the largest impact on a company's reputation?

#	Answer		Response	%
1	Data breach		23	35%
2	Government fines		1	2%
3	Public lawsuit		16	25%
4	Environmental accident		10	15%
5	Labor dispute		1	2%
6	Poor customer service		13	20%
7	Outsourcing		0	0%
8	Other		1	2%
	Total		65	100%

43. Where did you first hear about data breaches?

#	Answer		Response	%
1	News media (e.g. television, newspaper, radio, etc.)		151	70%
2	Family or friend		27	13%
3	Social Media		24	11%
4	Other		14	6%
	Total		216	100%

Other
letter
I heard about Ebay online in the news, I discovered Facebook and Yahoo breaches when my password wouldn't work
Class
Computer Sciences Class
this survey
internet
letter mailed
Review of bank statement
coworker
internet forums/ reddit
Online searches/Articles
I Have known they exist since childhood
Comapny
Financial company

44. How many stories about different data breaches have you seen/heard in the news media within the past three months?

#	Answer		Response	%
1	0		50	23%
2	1		50	23%
3	2		47	22%
4	3		30	14%
5	4		7	3%
6	5		3	1%
7	More than 5		29	13%
	Total		216	100%

45. Please review the following list of large data breaches that have occurred in the past few years. How many of these events are you aware of? Please select all that apply.

#	Answer		Response	%
1	Target		182	85%
2	JP Morgan Chase		48	22%
3	The Home Depot		93	43%
4	Snapchat		39	18%
5	Sony		100	47%
6	Nationwide Mutual Insurance		3	1%
7	Walgreens		22	10%
8	Facebook		54	25%
9	LinkedIn		10	5%
10	Adobe		15	7%
11	Twitter		15	7%
12	Ashley Madison		156	73%
13	Google Chrome		4	2%
14	None of the above		6	3%

46. How safe do you feel your personal information is at this moment in time?

#	Answer		Response	%
1	Extremely safe		3	1%
2	Very safe		51	24%
3	Somewhat safe		126	58%
4	Not safe		36	17%
	Total		216	100%

47. How threatened do you feel by hackers/data breachers at this moment in time?

#	Answer		Response	%
1	Extremely threatened		11	5%
2	Very threatened		24	11%
3	Somewhat threatened		121	56%
4	Not threatened		60	28%
	Total		216	100%

48. How vulnerable to identity theft do you feel at this moment in time?

#	Answer		Response	%
1	Extremely vulnerable		8	4%
2	Very vulnerable		26	12%
3	Somewhat vulnerable		139	64%
4	Not vulnerable		43	20%
	Total		216	100%

49. In general, how concerned are you about identity theft?

#	Answer		Response	%
1	Extremely concerned		15	7%
2	Very concerned		35	16%
3	Concerned		57	26%
4	Somewhat concerned		78	36%
5	Not concerned		31	14%
	Total		216	100%

50. What type of data security measures should companies devote the most resources towards?

#	Answer		Response	%
1	Preventative measures (e.g. encryption, cyber security)		195	90%
2	Reactive measures (e.g. credit monitoring for customers, breach management procedures)		19	9%
3	Other (please specify)		2	1%
	Total		216	100%

Other (please specify)
Both
It really should be both.

51. Do you think it is possible for companies to prevent data breaches?

#	Answer		Response	%
1	Yes		148	69%
2	No		68	31%
	Total		216	100%

52. Do you think a company that you do business with will have their data breached in the near future? (within three years)

#	Answer		Response	%
1	Yes		147	68%
2	No		69	32%
	Total		216	100%

53. Do you change your passwords regularly?

#	Answer		Response	%
1	Yes		119	55%
2	No		97	45%
	Total		216	100%

54. Did you change your passwords regularly before hearing about data breaches?

#	Answer		Response	%
1	Yes		76	64%
2	No		43	36%
	Total		119	100%

55. Do you use debit cards regularly?

#	Answer		Response	%
1	Yes		147	68%
2	No		69	32%
	Total		216	100%

56. Have you taken any security measures with regards to debit cards?

#	Answer		Response	%
1	Yes		61	41%
2	No		86	59%
	Total		147	100%

57. Were these changes in debit card security the result of hearing about data breaches?

#	Answer		Response	%
1	Yes		28	46%
2	No		33	54%
	Total		61	100%

58. Do you provide companies with your social security number regularly?

#	Answer		Response	%
1	Yes		29	13%
2	No		187	87%
	Total		216	100%

59. Did you regularly provide companies with your social security numbers before hearing about data breaches?

#	Answer		Response	%
1	Yes		13	7%
2	No		174	93%
	Total		187	100%

60. Do you use a personal data security service or program? (For example LifeLock and LastPass, internet firewall/security systems are not considered personal data security programs)

#	Answer		Response	%
1	Yes		40	19%
2	No		176	81%
	Total		216	100%

61. Did you use a personal data security service or program before hearing about data breaches?

#	Answer		Response	%
1	Yes		22	55%
2	No		18	45%
	Total		40	100%

62. Does the level of data security provided impact your decision to do business with a company?

#	Answer		Response	%
1	Yes, it impacts all of my decisions		23	11%
2	Yes, it impacts some of my decisions		146	68%
3	No		47	22%
	Total		216	100%

63. Do you feel prepared if a data breach were to happen to you?

#	Answer		Response	%
1	Yes		92	43%
2	No		124	57%
	Total		216	100%

64. What steps have you taken to protect yourself from identity theft? Please select all that apply.

#	Answer		Response	%
1	Done nothing		74	34%
2	Enrolled in an identity theft protection service		35	16%
3	Hired a paid service to monitor credit reports		11	5%
4	Closely monitor my credit reports		120	56%
5	Canceled credit/debit cards		42	19%
6	Canceled bank accounts		15	7%
7	Other (please specify)		6	3%

Other (please specify)
Do not use my debit card for purchases, just to get money from ATM since it would be more inconvenient if my debit card were breached
Limited where and when I use credit or debit cards
I use credit cards more and use my debit card only once in awhile.
closely monitor my bank accounts
I check my bank accounts no less than 5 times every day.
I have changed banks, but not because of worry. It makes me realize that i am not so prepared.

65. Gender

#	Answer		Response	%
1	Male		126	59%
2	Female		89	41%
	Total		215	100%

66. Age

#	Answer		Response	%
1	18 to 25		26	12%
2	26 to 35		90	42%
3	36 to 45		56	26%
4	46 to 55		27	13%
5	56 to 65		14	7%
6	66 to 75		2	1%
7	75+		0	0%
	Total		215	100%

67. Household Income Range

#	Answer		Response	%
1	Less than $25,000		42	20%
2	$25,000 to $40,000		50	23%
3	$40,001 to $60,000		47	22%
4	$60,001 to $80,000		31	14%
5	$80,001 to $100,000		22	10%
6	$100,000 to $150,000		18	8%
7	$150,000 to $250,000		4	2%
8	More than $250,000		1	0%
	Total		215	100%

68. Highest Level of Education

#	Answer		Response	%
1	Some High School		2	1%
2	High School		31	14%
3	Some College		63	29%
4	College (4 year degree)		87	40%
5	Post Graduate		30	14%
6	Doctorate		2	1%
	Total		215	100%

69. Ethnicity

#	Answer		Response	%
1	White/Caucasian		174	81%
2	Hispanic or Latino		5	2%
3	American Indian or Alaskan Native		1	0%
4	Asian		18	8%
5	Native Hawaiian or Pacific Islander		0	0%
6	Black/African American		15	7%
7	Unknown		2	1%
	Total		215	100%

70. Marital Status

#	Answer		Response	%
1	Single		108	50%
2	Married		92	43%
3	Divorced		15	7%
	Total		215	100%

71. Geographic Region

#	Answer		Response	%
1	Northeast		63	29%
2	Mid-Atlantic		10	5%
3	Midwest		51	24%
4	Southeast		51	24%
5	Southwest		22	10%
6	Pacific-West		18	8%
	Total		215	100%

72. Do you have identity fraud insurance?

#	Answer		Response	%
1	Yes		11	5%
2	No		204	95%
	Total		215	100%

73. Are you or a direct family member an identity theft victim?

#	Answer		Response	%
1	Yes		56	26%
2	No		159	74%
	Total		215	100%

Appendix B: Chi-Square Analysis

Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe... * Do you change your passwords regularly?

Crosstab

Count

		Do you change your passwords regularly?		
		Yes	No	Total
Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe...	Yes, me personally.	43_a	34_a	77
	Yes, someone I know.	40_a	34_a	74
	No.	36_a	29_a	65
Total		119	97	216

Each subscript letter denotes a subset of Do you change your passwords regularly? categories whose column proportions do not differ significantly from each other at the .05 level.

Chi-Square Tests

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	.052[a]	2	.974
Likelihood Ratio	.052	2	.974
Linear-by-Linear Association	.004	1	.948
N of Valid Cases	216		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 29.19.

Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe... * Did you change your passwords regularly before hearing about data breaches?

Crosstab

Count

		Did you change your passwords regularly before hearing about data breaches?		
		Yes	No	Total
Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe...	Yes, me personally.	27_a	16_a	43
	Yes, someone I know.	25_a	15_a	40
	No.	24_a	12_a	36
Total		76	43	119

Chi-Square Tests

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	.176[a]	2	.916
Likelihood Ratio	.177	2	.915
Linear-by-Linear Association	.118	1	.731
N of Valid Cases	119		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 13.01.

Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe... * Do you use debit cards regularly?

Crosstab

Count

		Do you use debit cards regularly?		
		Yes	No	Total
Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe...	Yes, me personally.	52_a	25_a	77
	Yes, someone I know.	51_a	23_a	74
	No.	44_a	21_a	65
Total		147	69	216

Each subscript letter denotes a subset of Do you use debit cards regularly? categories whose column proportions do not differ significantly from each other at the .05 level.

Chi-Square Tests

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	.039[a]	2	.981
Likelihood Ratio	.039	2	.981
Linear-by-Linear Association	.001	1	.976
N of Valid Cases	216		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 20.76.

Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe... * Have you taken any security measures with regards to debit cards?

Crosstab

Count

		Have you taken any security measures with regards to debit cards?		
		Yes	No	Total
Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe...	Yes, me personally.	24_a	28_a	52
	Yes, someone I know.	23_a	28_a	51
	No.	14_a	30_a	44
Total		61	86	147

Each subscript letter denotes a subset of Have you taken any security measures with regards to debit cards? categories whose column proportions do not differ significantly from each other at the .05 level.

Chi-Square Tests

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2.435[a]	2	.296
Likelihood Ratio	2.480	2	.289
Linear-by-Linear Association	1.910	1	.167
N of Valid Cases	147		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 18.26.

Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe... * Were these changes in debit card security the result of hearing about data breaches?

Crosstab

Count

		Were these changes in debit card security the result of hearing about data breaches?		
		Yes	No	Total
Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe...	Yes, me personally.	15_a	9_b	24
	Yes, someone I know.	10_a	13_a	23
	No.	3_a	11_b	14
Total		28	33	61

Each subscript letter denotes a subset of Were these changes in debit card security the result of hearing about data breaches? categories whose column proportions do not differ significantly from each other at the .05 level.

Chi-Square Tests

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.094[a]	2	.048
Likelihood Ratio	6.358	2	.042
Linear-by-Linear Association	5.981	1	.014
N of Valid Cases	61		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 6.43.

Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe... * Do you provide companies with your social security number regularly?

Crosstab

Count

		Do you provide companies with your social security number regularly?		
		Yes	No	Total
Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe...	Yes, me personally.	16_a	61_b	77
	Yes, someone I know.	9_a	65_a	74
	No.	4_a	61_b	65
Total		29	187	216

Each subscript letter denotes a subset of Do you provide companies with your social security number regularly? categories whose column proportions do not differ significantly from each other at the .05 level.

Chi-Square Tests

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.641[a]	2	.036
Likelihood Ratio	6.851	2	.033
Linear-by-Linear Association	6.540	1	.011
N of Valid Cases	216		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 8.73.

Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe... * Did you regularly provide companies with your social security numbers before hearing about data b...

Crosstab

Count

		Did you regularly provide companies with your social security numbers before hearing about data b...		
		Yes	No	Total
Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe...	Yes, me personally.	3_a	58_a	61
	Yes, someone I know.	5_a	60_a	65
	No.	5_a	56_a	61
Total		13	174	187

Each subscript letter denotes a subset of Did you regularly provide companies with your social security numbers before hearing about data b... categories whose column proportions do not differ significantly from each other at the .05 level.

Chi-Square Tests

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	.591[a]	2	.744
Likelihood Ratio	.624	2	.732
Linear-by-Linear Association	.504	1	.478
N of Valid Cases	187		

a. 3 cells (50.0%) have expected count less than 5. The minimum expected count is 4.24.

Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe... * Do you use a personal data security service or program? (For example LifeLock and LastPass, inter...

Crosstab

Count

		Do you use a personal data security service or program? (For example LifeLock and LastPass, inter...		
		Yes	No	Total
Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe...	Yes, me personally.	17_a	60_a	77
	Yes, someone I know.	16_a	58_a	74
	No.	7_a	58_a	65
Total		40	176	216

Chi-Square Tests

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	3.706[a]	2	.157
Likelihood Ratio	4.020	2	.134
Linear-by-Linear Association	2.823	1	.093
N of Valid Cases	216		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 12.04.

Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe... * Did you use a personal data security service or program before hearing about data breaches?

Crosstab

Count

		Did you use a personal data security service or program before hearing about data breaches?		
		Yes	No	Total
Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe...	Yes, me personally.	6_a	11_b	17
	Yes, someone I know.	11_a	5_a	16
	No.	5_a	2_a	7
Total		22	18	40

Each subscript letter denotes a subset of Did you use a personal data security service or program before hearing about data breaches? categories whose column proportions do not differ significantly from each other at the .05 level.

Chi-Square Tests

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4.653[a]	2	.098
Likelihood Ratio	4.726	2	.094
Linear-by-Linear Association	3.710	1	.054
N of Valid Cases	40		

Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe... * Does the level of data security provided impact your decision to do business with a company?

Crosstab

Count

		Does the level of data security provided impact your decision to do business with a company?			
		Yes, it impacts all of my decisions	Yes, it impacts some of my decisions	No	Total
Have you, or someone you know, been affected by a data breach? Remember, that a data breach refe...	Yes, me personally.	12_a	49_a	16_a	77
	Yes, someone I know.	5_a	53_a	16_a	74
	No.	6_a	44_a	15_a	65
Total		23	146	47	216

Each subscript letter denotes a subset of Does the level of data security provided impact your decision to do business with a company? categories whose column proportions do not differ significantly from each other at the .05 level.

Chi-Square Tests

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	3.380[a]	4	.496
Likelihood Ratio	3.321	4	.506
Linear-by-Linear Association	.906	1	.341
N of Valid Cases	216		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 6.92.

Appendix C: ANOVA Analysis of Sentiment

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
How safe do you feel your personal information is at this moment in time?	Between Groups	3.199	2	1.600	3.634	.028
	Within Groups	93.759	213	.440		
	Total	96.958	215			
How threatened do you feel by hackers/data breachers at this moment in time?	Between Groups	3.058	2	1.529	2.625	.075
	Within Groups	124.035	213	.582		
	Total	127.093	215			
How vulnerable to identity theft do you feel at this moment in time?	Between Groups	2.519	2	1.260	2.725	.068
	Within Groups	98.476	213	.462		
	Total	100.995	215			
In general, how concerned are you about identity theft?	Between Groups	1.892	2	.946	.749	.474
	Within Groups	269.067	213	1.263		
	Total	270.958	215			

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
How safe do you feel your personal information is at this moment in time?	Yes, me personally.	77	3.05	.724	.082	2.89	3.22	1	4
	Yes, someone I know.	74	2.88	.661	.077	2.73	3.03	1	4
	No.	65	2.75	.587	.073	2.61	2.90	1	4
	Total	216	2.90	.672	.046	2.81	2.99	1	4
How threatened do you feel by hackers/data breachers at this moment in time?	Yes, me personally.	77	2.99	.752	.086	2.82	3.16	1	4
	Yes, someone I know.	74	2.99	.868	.101	2.79	3.19	1	4
	No.	65	3.25	.638	.079	3.09	3.40	1	4
	Total	216	3.06	.769	.052	2.96	3.17	1	4
How vulnerable to identity theft do you feel at this moment in time?	Yes, me personally.	77	2.94	.675	.077	2.78	3.09	1	4
	Yes, someone I know.	74	2.93	.746	.087	2.76	3.11	1	4
	No.	65	3.17	.601	.075	3.02	3.32	2	4
	Total	216	3.00	.685	.047	2.91	3.10	1	4
In general, how concerned are you about identity theft?	Yes, me personally.	77	3.36	1.038	.118	3.13	3.60	1	5
	Yes, someone I know.	74	3.23	1.222	.142	2.95	3.51	1	5
	No.	65	3.46	1.105	.137	3.19	3.74	1	5
	Total	216	3.35	1.123	.076	3.20	3.50	1	5